Department of Homeland Security Daily Open Source Infrastructure Report for 01 February 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Los Angeles Times reports seven of the largest tunnels discovered under the U.S.−Mexico border in recent years have yet to be filled in, raising concerns because smugglers have tried to reuse such passages before. (See item 17)
- The Government Accountability Office has published a Special Report entitled, High−Risk Series: An Update, which included audits and evaluations that identify federal programs and operations that are high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement. (See item 25)
- The Maryland Coordination and Analysis Center is one of about 20 state, local, or regional "intelligence fusion centers" that will gather representatives from law enforcement along with intelligence analysts and representatives from federal agencies to work under one roof. (See item 26)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *January 31, Government Accountability Office* — **GAO−07−36: National Nuclear Security Administration: Additional Actions Needed to Improve Management of the Nation's**

Nuclear Programs. In response to security and management weaknesses, in 1999 the Congress created the National Nuclear Security Administration (NNSA). Since its creation, NNSA has continued to experience security problems, such as unauthorized access to a NNSA unclassified computer system, and cost and schedule overruns on its major projects, such as the National Ignition Facility. The Government Accountability Office (GAO) reviewed the extent to which NNSA has taken steps to (1) improve security at its laboratories and plants and (2) improve its management practices and revise its organizational structure. GAO is recommending that the Secretary of Energy and the Administrator, NNSA, (1) improve NNSA's security program, (2) develop and implement standard operating procedures for conducting business and resolving conflicts between the Department of Energy and NNSA, and (3) institute a series of initiatives to improve project, program, and financial management. NNSA generally agreed with the report's findings and corresponding recommendations.
Highlights: http://www.gao.gov/highlights/d0736high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−36

2. *January 30, Reuters* — **U.S. refiners make gasoline early amid winter warmth.** U.S. oil refineries are producing and storing summer−grade gasoline earlier than usual after a warm start to winter left the market awash with heating oil, traders and analysts said. The early focus on gasoline production well ahead of the summer driving season may add to stockpiles which already exceed the upper end of the average range, though some experts expect heavy spring refinery maintenance could counter the supply jump by slicing into overall fuel production. Tight gasoline stocks in 2006 were a key factor behind crude oil's rise above $78 a barrel in July. "Refiners are making more gasoline than we normally expect them to make in the winter," said Doug MacIntyre, analyst at the Energy Information Administration. "It appears to be the case that refiners are emphasizing the production of gasoline earlier than usual because of the mild winter," said John Kilduff of Fimat USA. Robust gasoline output from U.S. refineries and strong imports from Europe have combined to boost gasoline stocks by nearly 20 million barrels since mid−December, bringing them to 24.2 days of U.S. demand from 23.9 days a year ago.
Source: http://today.reuters.com/news/articlenews.aspx?type=reutersEdge&storyID=2007−01−30T193713Z_01_N29205597_RTRUKOC_0_US−REFINERY−OPERATIONS−USA.xml&from=business

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *January 31, U.S. Air Force* — **Air Force posts KC−X request for proposals.** The assistant secretary of the Air Force for acquisition announced Tuesday, January 30, the posting of the KC−X Aerial Refueling Aircraft Request for Proposal (RFP) to the Federal Business Opportunities Website, signaling the official launch of the Air Force's No. 1 priority acquisition

program. The announcement comes after an extensive and transparent dialogue between Air Force officials and officials from the office of the secretary of defense, Air Mobility Command, industry and members of Congress. Sue C. Payton, the Air Force's senior acquisition executive, said that throughout this entire acquisition process, the Air Force has sought to minimize development risk among differing aircraft manufacturers and types. This RFP is the culmination of those deliberations.
Source: http://www.af.mil/news/story.asp?storyID=123039360

4. *January 31, Washington Post* — **IG report: Flaws found in government oversight of contractors in Iraq.** The U.S. government has squandered millions of dollars intended for police training programs in Iraq because of rampant problems overseeing contractors, according to federal reviews released Tuesday, January 30. In one case, contractors building a camp for American trainers constructed an Olympic−size swimming pool that hadn't been ordered. In another, human waste reportedly continues to leak from plumbing fixtures at a barracks for Iraqi police recruits, a year after the problem was first identified and despite assurances from the contractor that the problem was being fixed. While Tuesday's reports by the special inspector general for Iraq reconstruction do not address the training itself, they do find major flaws with how both the government and its contractors attempted to build the program's facilities. The flaws, auditors concluded, all had common roots: The government's failure to monitor how contractors were spending taxpayer money.
IG Report: http://www.sigir.mil/reports/quarterlyreports/Jan07.aspx
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/01/30/AR2007013001801.html

[Return to top]

Banking and Finance Sector

5. *January 31, VNUNet* — **Cyber−crooks take aim at online games.** Cyber−criminals are increasingly targeting online games in an effort to rob players of virtual assets and sell them on auction Websites. Trend Micro identified more than 3,600 spyware attacks last year designed to gather log−in and password information for online games such as Second Life, Lineage, and World of Warcraft. The password stealers are often spread through spam messages where they are presented as virtual goods or popular media content such as music or movie files. The thieves can then auction off virtual currencies and accessories such as clothing and weapons.
Source: http://www.vnunet.com/vnunet/news/2173816/online−criminals−a im−online

6. *January 31, China Daily* — **For Chinese hackers, it's a game.** Money is by far the primary motivation for most of today's virus writing and spamming in the world of computers except when it comes to China. For Chinese hackers, gaming prestige outweighs financial gain, according to a new report on Internet security. The target of Chinese Internet malicious software, or malware, is to steal better online weapons and the profiles of the most famous gamers. According to Sophos' Security Threat Report 2007, Chinese hackers accounted for 30 percent of the malware written last year, surpassed only by the U.S. The report also reveals some national characteristics of hackers. Brazilian hackers tend to produce simulations of banks' Websites, attempting to get your credit card information; while hackers from Russia and Sweden create backdoors to vulnerable computers. The motivation is financial gain. In contrast,

the Chinese malware aims at "health", "power" and gaming profiles.
Source: http://english.peopledaily.com.cn/200701/31/print20070131_34 6292.html

7. *January 31, Associated Press* — **U.S. suspects North Korea laundering money.** A U.S. Treasury envoy who on Wednesday, January 31, wrapped up two days of talks with North Korean officials said his agency's suspicions of illegal financial activity involving bank accounts linked to the communist nation were accurate. Deputy Assistant Treasury Secretary Daniel Glaser said that he went over bank information of 50 account holders from the Macao−based Banco Delta Asia with his North Korean counterparts in Beijing, adding that U.S. concerns that the bank was being used for money−laundering purposes had "been vindicated" by the discussions. Glaser said the two sides planned to meet again to talk further about U.S. financial restrictions imposed due to Pyongyang's alleged smuggling and counterfeiting, but no date had been set. Washington took action against the Banco Delta Asia in 2005, accusing the bank of complicity in North Korea's alleged illegal financial activity such as counterfeiting and money−laundering. The move has caused other banks to steer clear of North Korean business for fear of losing access to the U.S. market, hampering the North's access to the international financial system.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/01/31/AR2007013100692.html

8. *January 30, KCRA 3 (CA)* — **Suspected ID theft ring leader arrested.** A man investigators described as the suspected leader of an identity theft ring with crimes dating back more than a decade has been arrested. Tien Nguyen was arrested Friday, January 26, by the Placer County, California Sheriff's Department and the U.S. Secret Service. Prosecutors said they believe Nguyen organized a large identity theft ring that stole personal credit card information using phishing scams. More than 1,000 victims have already come and even more are expected. "We don't get to people at his level hardly ever. People like him usually isolate themselves from law enforcement using lesser people in order to conduct the theft itself, and then he usually profits from it," Placer County Sheriff's Department spokesperson Jim Hudson said. Seven other arrests were made in connection with the same ring late last year.
Source: http://www.kcra.com/news/10873806/detail.html?subid=22100408 &qs=1;bp=t

9. *January 30, eWeek* — **Data security firms ally to promote standards.** Eight leading data security companies have joined forces to create an organization to educate the business community on the value of global security standards that protect credit and debit card numbers. The newly formed Payment Card Industry Security Vendor Alliance will assist the PCI Security Standards Council—an organization composed of merchants, banks and point−of−sale vendors—in educating the business community on the requirements and business value of the Payment Card Industry Data Security Standard. The data security standard—a series of rules commonly called the "digital dozen"—sets requirements for security management, network architecture, software design and other critical protective measures. Each of the founding members of PCI SVA—ConfigureSoft, Cyber−Ark, Modulo Security, Proginet, Protegrity USA, Reflex Security, SafeNet and Verisign—will provide flexible PCI Data Security Standard solutions to address the needs of system integrators and business users.
Source: http://www.eweek.com/article2/0,1895,2088739,00.asp

[Return to top]

Transportation and Border Security Sector

10. *January 31, Associated Press* — **Suspicious luggage leads to delays.** Hundreds of commuters who use the Washington, DC area's transit system endured delays Wednesday morning, January 31, because of a delayed investigation of suspicious items found near a Metrorail station just outside the nation's capital. The items had been abandoned and not deemed a threat. About 3 a.m. EST a Metro employee saw two suitcases and a backpack near the bus waiting area of the Braddock Road station in Alexandria. But the items sat there for at least two hours because the city's police do not have a bomb squad and "apparently, they couldn't get a hold of anybody from Metro (police) until after 5 a.m.," Alexandria police Lt. James Bartlett said. Metro spokesperson Cathy Asato said the delay in locating Metro transit police "is something that we will look into." By 7 a.m., Metro's bomb squad had arrived at the Braddock Road station.
Source: http://www.wusa9.com/news/news_article.aspx?storyid=55464

11. *January 31, New York Times* — **US Airways withdraws Delta offer.** US Airways said Wednesday, January 31, that it would withdraw its $10.2 billion offer to acquire Delta Air Lines out of bankruptcy after the offer failed to win the support of the official committee of Delta's creditors. The move marked a victory for Delta's management and its pilots' union, both of which have repeatedly said that Delta should pursue a plan that allows to exit Chapter 11 protection as an independent airline. US Airways, of Tempe, AZ, had said that its offer would expire Thursday unless Delta's creditors asked the airline open its books so it could perform due diligence and took other steps to delay Delta's reorganization plan. In a statement Wednesday, however, the creditors' committee said it was backing Delta's standalone plan. US Airways chief executive W. Douglas Parker said that he continued to believe a merger would provide more value for Delta's creditors and suggested that Delta's creditors committee had overstated concerns about such a deal. Delta has raised concerns about potential antitrust problems and the debt that a combined Delta−US Airways would carry.
Source: http://dealbook.blogs.nytimes.com/2007/01/31/delta−committee−backs−standalone−plan/

12. *January 31, Boston Globe* — **MBTA bag searches turn up no weapons, arrests, but some false alarms.** In the first two and one−half months of random bag searches on the Massachusetts Bay Transit Authority (MBTA), police found no weapons, made no arrests, but had nearly two−dozen false alarms for explosives. Of the 2,449 inspections between October 10 and December 31, the bags of 27 riders tested positive in the initial screening for explosives, prompting further searches. In the additional screening, 11 passengers had their bags checked by explosive−sniffing dogs, and 16 underwent a physical search. Nothing was found. Still, MBTA officials said the searches have been effective at thwarting potential terrorists and have been supported by passengers. Daniel A. Grabauskas, MBTA general manager said, "Every single organized terrorist action that we have been able to dissect . . . demonstrated that the terrorists rehearsed and counted on the fact that there was predictability in the system that would allow them to carry out a very defined plan."
Source: http://www.boston.com/news/local/articles/2007/01/31/ts_searches_turn_up_only_false_alarms/

13.

January 31, Eureka Reporter (CA) — **Ticking package causing evacuation turns out to be box of toys.** Eureka, CA, police and bomb experts from the Humboldt County Sheriff's Office spent Tuesday morning, January 30, making sure a suspicious ticking package at the Clark Street post office was not a bomb. Shortly after 6:45 a.m. PST, police responded to the post office after postal employees reported a suspicious package on the loading dock. Postal employees told police they had discovered a package in the normal flow of mail that was ticking and had evacuated all personnel from the building and called the Eureka Police Department. The sender and recipient of the package, which was being sent to Trinidad from Connecticut, were eventually contacted and indicated that there were toys in the box. As a precaution, Explosive Ordinance Device experts took an X−ray of the package and confirmed that it was harmless, a release stated. A situation such as this is easily preventable, said Augustine Ruiz, USPS spokesperson for Northern California. "By and large, people that send toys or any device that requires a battery … they should always pack them in the same box, but removed," he said. If a battery is in a device, Ruiz said it is not uncommon for the device to turn on.
Source: http://www.eurekareporter.com/ArticleDisplay.aspx?ArticleID= 19972

14. *January 31, KGO TV (CA)* — **Flight safety clashes with San Jose skyline.** The business community in downtown San Jose, CA, is going up against airlines over plans for new high−rises that could stand in the way of growing Mineta San Jose International Airport. This is a battle for expanding business, with safety issues tossed into the mix. Developers have plans to build more high−rises in downtown San Jose, but airport officials are protesting, claiming flight path problems and their own potential loss of business. A consultant hired by the Mineta San Jose International Airport points to at least a dozen planned high−rise developments that could interfere with a jet's emergency route. San Jose's downtown buildings meet federal safety standards −− the problem is the need for emergency routes available after takeoff from the airport. The study indicates that emergency routes will fewer if the new buildings keep getting taller. Their recommendation is to trim them down. City officials estimate the economic impact of trimming a building could be an annual tax revenue loss of up to one million dollars. On the other hand, if an airline decides not to operate just one future long−haul flight because of a dangerous skyline, the economic impact could be more than $20−million dollars.
Source: http://abclocal.go.com/kgo/story?section=local&id=4988703

15. *January 31, WUSA9 (DC)* — **Washington, DC Metro bus explosion.** Metro says a problem with braking and air drying systems caused Wednesday, January 31's, fire on a bus as it was traveling through downtown Washington, DC. Three passengers and a driver were on the bus when the explosion occurred. The people were able to get off the bus before the fire intensified. Personnel from the DC Fire and Emergency Medical Services Department quickly extinguished the flames.
Source: http://www.wusa9.com/news/news_article.aspx?storyid=55452

16. *January 31, Associated Press* — **Boston suspicious devices called a hoax.** Five suspicious packages planted near bridges and other spots around Boston forced the shutdown of major roads, a bridge and a stretch of the Charles River on Wednesday, January 31, before authorities concluded the objects were not bombs. Police said four calls, all around 1 p.m. EST, reported suspicious devices at the Boston University Bridge and the Longfellow Bridge −− which both span the Charles River −− at a Boston street corner and at the Tufts−New England Medical

Center. The package near the Boston University bridge was found attached to a structure beneath the span, where it crosses the Massachusetts Turnpike, authorities said. Subway service across the Longfellow Bridge between Boston and Cambridge was briefly suspended, and Storrow Drive was closed as well. Another device was found earlier in the day at a subway station, forcing a temporary shutdown of Interstate 93.
Source: http://www.baltimoresun.com/news/nationworld/bal−boston0131,0,465748.story?coll=bal−nationworld−headlines

17. *January 30, Los Angeles Times* — **Unfilled tunnels a weak link at border.** Seven of the largest tunnels discovered under the U.S.−Mexico border in recent years have yet to be filled in, authorities said, raising concerns because smugglers have tried to reuse such passages before. Among the unfilled tunnels, created to ferry people and drugs, is the longest one yet found −− extending nearly half a mile from San Diego to Tijuana. Nearby, another sophisticated passageway once known as the Taj Mahal of tunnels has been sitting unfilled for 13 years, authorities say. Though concrete plugs usually close off the tunnels where they cross under the border and at main entrance and exit points, the areas in between remain largely intact. Filling the seven tunnels would cost about $2.7 million, according to U.S. Customs and Border Protection officials. Mexican authorities have told their U.S. counterparts that they've filled their end of the tunnels. But U.S. officials express doubt, citing the high costs and examples of tunnels being compromised. But smugglers in some cases have been able to access existing tunnels by digging around the plugged entrance points, according to the U.S. Border Patrol and Immigration and Customs Enforcement, which heads the San Diego−based U.S. Border Tunnel Task Force.
Source: http://www.latimes.com/news/printedition/la−me−tunnel30jan30,1,7265573.story?ctrack=1&cset=true

18. *January 30, Gov Exec* — **Coast Guard modernization program faces increased oversight.** Coast Guard Commandant Adm. Thad Allen told lawmakers Tuesday, January 30, he would hold agency personnel and contractors accountable for improving performance in the service's troubled modernization program known as Deepwater. In testimony before the House Transportation and Infrastructure Subcommittee on the Coast Guard and Maritime Transportation, Allen acknowledged serious problems with the mammoth program to replace its aging equipment. The program is being run by the Integrated Coast Guard Systems, a joint venture of defense contractors Lockheed Martin and Northrop Grumman. Allen said he took seriously a withering report on the acquisition of the National Security Cutter, the cornerstone of the Deepwater fleet, by Richard Skinner, the inspector general of the Homeland Security Department, the Coast Guard's parent agency. According to Skinner's 133−page report, the cutter will not meet the performance specifications described in the Deepwater contract. Moreover, he said, the Coast Guard had abdicated its oversight authority in deference to the contractors. Rep. Elijah E. Cummings, (D−MD), subcommittee chair, plans to call Allen as a witness again in 120 days to discuss progress on Deepwater.
Source: http://www.govexec.com/story_page.cfm?articleid=35992&dcn=to daysnews

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

19. *January 31, USAgNet* — **Winter storm stress on plains cattle continues.** Even after spring arrives, this winter's storms in the Plains will continue to be felt by severely stressed cows and calves, a Kansas State University veterinarian said. Heavy snow and bitter cold from a string of storms have killed thousands of cattle in Colorado and the southern Plains this winter. The effects of the wintry weather stress could last all the way until it is time to re−breed cows, Larry Hollis, KSU Research and Extension veterinarian, said. Hollis said he is concerned about "secondary losses," which he characterized as weak calves at birth, cows that are in poorer condition than usual during calving season, and the possibility that severely stressed cows could cut conception rates amid lack of fertility at re−breeding time, reports the Dow Jones News Service. Much will depend upon how many days cattle went without feed, he said. Animals that went without feed for one or more period over the last several weeks used up body reserves, which would make them even more vulnerable to cold snaps, he said. A cold snap can sometimes spark spontaneous abortions in an already−stressed cow within 48 hours of the drop in temperatures, Hollis said.
Source: http://www.usagnet.com/story−national.php?Id=255&yr=2007

20. *January 30, Dow Jones* — **Antibiotic resistance still rising.** Disease resistance to antibiotics among humans and animals continues to rise, despite declines in their use as a feed−ration additive to prevent illness and to promote growth in livestock and poultry, according to scientists and livestock industry members. In addition, worldwide use of antibiotics to treat sick animals has increased in the last seven years, but total use remains below mid−1990s peaks, according to statistics for Europe by the Danish government. The U.S. situation −− declines in feed use to promote general herd or flock health and as a growth promoter −− corresponds to an increase in therapeutic use to treat a higher numbers of sick animals or birds. It "is precisely what is taking place in Europe," said Ron Phillips, vice president of legislative and public affairs for the Animal Health Institute, citing figures from the Danish government's program for surveillance of European antimicrobial resistance. The report for 2005, the most recent statistics available, says, "antimicrobial consumption in food animals is still low compared to the total consumption before the cessation of growth promoter use." In the U.S., subtherapeutic antibiotic use, or below the level required to cure a sick animal, in livestock and poultry feed has declined in the last three years, Phillips said.
Source: http://www.cattlenetwork.com/content.asp?contentid=101853

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

21. *January 30, Tallahassee Democrat (FL)* — **Tallahassee water−security plan has a few holes.** Tallahassee, FL, has a plan in place to protect the city's water supply in case of a terrorist attack, but it has a few holes, a recent audit found. Among its findings, the audit noted that: some city employees weren't properly notified of what would be expected of them in an emergency; the locations of valves needed to isolate the water supply weren't identified in the emergency plan and access to a city wastewater plant was too lax. The emergency plan was developed as a result of the federal 2002 Bioterrorism Act, which mandated that all water utilities serving more than 3,300 customers develop vulnerability assessments in the wake of the September 11 attacks. The city has appropriated $1.050 million for security improvements, about a third of which had been used as of August 31, 2006, according to the audit.
Audit Report: http://www.tallahassee.com/assets/pdf/CD59169126.PDF
Source: http://www.tallahassee.com/apps/pbcs.dll/article?AID=/20070130/NEWS01/701300323

[Return to top]

Public Health Sector

22. *January 30, Agence France−Presse* — **Japan steps up measures to counter bird flu.** Japan has announced new measures to combat bird flu after four cases in the past month, as another recent outbreak was confirmed to be the virulent H5N1 strain of the virus. The farm ministry said it had formed an emergency task force to strengthen prevention measures and would back sending troops to help anti−flu efforts in worst−hit southwestern Miyazaki prefecture. "The farm ministry would support Miyazaki prefecture if it calls for the deployment of the Self−Defense Forces," Farm Minister Toshikatsu Matsuoka said, referring to officially pacifist Japan's military. Matsuoka will head the emergency task force, which includes experts in poultry disease and meet on potential new measures against bird flu. In the latest suspected outbreak reported Tuesday, January 30, a total of 23 birds were found dead at a poultry farm in the town of Shintomicho in Miyazaki prefecture. Two cases of the virulent H5N1 strain were detected earlier in January in Miyazaki prefecture and a third case of bird flu was reported Monday, January 29, in western Okayama prefecture. A laboratory confirmed Wednesday, January 31, that the case in Okayama prefecture was also H5N1.
Source: http://news.yahoo.com/s/afp/20070131/hl_afp/healthflujapan_0 70131044557

23. *January 30, East African Standard (Kenya)* — **Kenya: Nairobi put on alert over Rift Valley fever.** Nairobi, Kenya, has now been put on alert and declared a high−risk area under the threat of a possible Rift Valley fever outbreak, the Government has announced. The Director of Medical Services and the Director of Veterinary Services will hold a media conference on the safety of meat in the city on Wednesday, January 31. Livestock Minister Joseph Munyao announced that Nairobi had joined nine other districts where possibilities for the disease outbreak are high. The others are Nakuru, Koibatek, Uasin Gichu, Trans Nzoia, Trans Mara, Narok, Kajiado, and Machakos. "Based on disease outbreak historical dates, 10 districts have been identified for vaccination using the available one million doses of Rift Valley fever vaccine," Munyao said. A source from the Ministry of Health has said at least 120 people have died since the outbreak was reported in December last year while 400 cases have been reported.
Rift Valley fever information: http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/rvf.htm

Source: http://allafrica.com/stories/200701300869.html

24. *January 30, Associated Press* — **Outbreak suspends high school wrestling statewide.** High school wrestling was suspended Tuesday, January 30, across Minnesota due to a widespread outbreak of a skin infection. The Minnesota State High School League said 24 cases of herpes gladiatorum have been reported by 10 teams. The virus is spread by skin−to−skin contact. The league banned competitions and direct contact between wrestlers in practice until Tuesday, February 6. The Minnesota Department of Health has been tracking the virus, caused by herpes simplex type 1, the same strain that causes cold sores. League officials first became aware of the outbreak at a tournament held in Rochester in late December.
Source: http://www.macon.com/mld/macon/sports/colleges/mercer/165809 05.htm

[Return to top]

Government Sector

25. *January 31, Government Accountability Office* — **GAO−07−310: High−Risk Series: An Update (Special Report).** The Government Accountability Office's (GAO) audits and evaluations identify federal programs and operations that, in some cases, are high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement. In recent years, GAO also has identified high−risk areas to focus on the need for broad−based transformations to address major economy, efficiency, or effectiveness challenges. Since 1990, GAO has periodically reported on government operations it has designated as high risk. In this 2007 update for the 110th Congress, GAO presents the status of high−risk areas identified in 2005 and new high−risk areas warranting attention by Congress and the executive branch. Lasting solutions to high−risk problems offer the potential to save billions of dollars, dramatically improve service to the public, strengthen confidence and trust in the performance and accountability of the U.S. government, and ensure the ability of government to deliver on its promises. This report contains GAO's views on what remains to be done to bring about lasting solutions for each high−risk area. Perseverance by the executive branch in implementing GAO's recommended solutions and continued oversight and action by Congress are both essential to achieving and sustaining progress
Highlights: http://www.gao.gov/highlights/d07310high.pdf
Source: http://www.gao.gov/new.items/d07310.pdf

[Return to top]

Emergency Services Sector

26. *February 01, National Defense* — **Fusion centers aim to connect federal, state, local agencies.** The Maryland Coordination and Analysis Center (MCAC) is one of about 20 state, local or regional "intelligence fusion centers" that has received Department of Homeland Security (DHS) funding. The concept calls for states, regions or cities to gather representatives from all their law enforcement agencies under one roof, along with intelligence analysts and representatives from federal agencies. Charles Allen, DHS intelligence officer, said if there is pertinent information, the department will find a way to quickly push it down to the appropriate

officials, regardless of whether they have a fusion center. For top secret documents, DHS, Justice and the Defense Department are forming a federal coordinating group at the National Counterterrorism Center to find ways to vet source material for local officials. Allen is also leading efforts to install the classified homeland security data network terminals at fusion centers, or other state and local law enforcement offices. Among the systems MCAC is using is the Defense Department's secret Internet protocol router network (SIPRNET), DHS' homeland security information network (HSIN) and the Justice Department's Guardian system. The HSIN allows the center to link to other state and local fusion centers.
MCAC Website: http://www.mcac−md.gov/
Maryland Governor's Office of Homeland Security:
http://www.gov.state.md.us/gohs/gohs_initiatives.html
Source: http://www.nationaldefensemagazine.org/issues/2007/Febuary/F usioncenters.htm

27. *January 31, Ledger Dispatch (CA)* — **Preparing for an emergency.** There are many things to consider when a disaster occurs but almost always there is no time to think when one is actually happening. On Saturday, January 27, a variety of local and state organizations gathered at the second annual Disaster Preparedness Fair hosted by the Amador Fire Safe Council and the Amador Chapter American Red Cross in Amador County, CA. The fair helped educate county residents on ways to prepare so that if and when a disaster should occur, they will be ready. The event included about 14 booths from organizations like Amador County Sheriff Search and Rescue, the Amador County Health Department, and the U.S. Forest Service and also included insurance companies. Outside of the building, Sutter Amador Hospital Emergency Management Coordinator Joyce Friday set up a mini−disaster triage area to show people how the hospital would organize itself in the event of a disaster. Besides preparing people for disasters, a few groups were present to help people learn what to do with their pets and farm animals should a flood, earthquake, fire or other emergency occur.
Source: http://www.ledger−dispatch.com/news/newsview.asp?c=204888

28. *January 31, Firehouse.Com* — **Texas volunteers provide valuable community assistance.** The College Station Fire Department, located in southeast Texas, is home to a group of dedicated Fire Corps volunteers who serve on the department's Community Action Response Team (CART). CART was established in 2002 by the College Station Fire Department to provide customer assistance and emotional support to residents who are dealing with stressful situations following a fire or other emergency that requires a resident to evacuate their home. The Community Action Response Team is staffed by 25 volunteers who are graduates of the College Station Citizen's Fire Academy. In College Station, the Citizens Fire Academy is a 14−week class which provides our citizens with in−depth training about the fire department and their own safety. Members of the team take monthly rotation schedules and are alerted by our 911 dispatchers through the fire department paging system. The team provides fire victims with ongoing assistance such as recovery information, shelter, packing boxes, clothes or any other needed services during and after an incident.
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=9&id=53143

[Return to top]

Information Technology and Telecommunications Sector

29. *January 31, SecurityFocus* — **Microsoft Word 2003 unspecified code execution vulnerability.** Microsoft Word 2003 is prone to an unspecified remote code−execution vulnerability. Microsoft Word 2003 is confirmed vulnerable to an unspecified remote code−execution issue. Although it has not been confirmed, other versions of Microsoft Word/Office may be affected by the vulnerability. Note that this issue is distinct from the Microsoft Word 2000 unspecified code execution vulnerability. Currently, SecurityFocus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/22328/discuss

30. *January 31, Sophos* — **Dorf malware storms the top ten chart.** Sophos has revealed the most prevalent malware threats and e−mail hoaxes causing problems for computer users around the world during January 2007. The figures show that the recently discovered Dorf malware has had a massive impact on computer users worldwide, rampaging to the top of the monthly malware threat chart and accounting for almost 50 percent of all malware seen during January. The Dorf malware was aggressively spammed out posing as breaking news of deaths caused by stormy European weather during January. Later in the month the authors changed tack and launched a further campaign disguising the malware as a romantic e−mail greeting card. Elsewhere in the top ten, the Netsky, Mytob and Stratio malware remain rooted in second, third and fourth place respectively, between them accounting for one third of all malware reports. View source for full report.
Source: http://www.sophos.com/pressoffice/news/articles/2007/01/topt enjan07.html

31. *January 31, IDG News Service* — **U.S. government does poorly in cybersecurity.** The Cyber Security Industry Alliance (CSIA) has given the U.S. government D grades on its cybersecurity efforts in 2006, and renewed its call for the Congress to pass a comprehensive data protection law in 2007. The CSIA, a trade group representing cybersecurity vendors, gave the U.S. government D grades in three areas: security of sensitive information, security and reliability of critical infrastructure, and federal government information assurance. In addition to a comprehensive data protection bill, CSIA called for the U.S. government to strengthen the power of agency chief information officers and called on agencies to increase testing of cybersecurity controls.
Report: https://www.csialliance.org/resources/pdfs/CSIA_06Report_07A genda_US_Govt.pdf
Source: http://www.infoworld.com/article/07/01/31/HNlowcybergrades_1 .html

32. *January 30, IDG News Service* — **Porn marketer settles spam charges with FTC.** An Internet−based provider of sexually explicit entertainment has agreed to pay a $465,000 civil penalty for sending unwanted e−mail, the U.S. Federal Trade Commission (FTC) announced Tuesday, January 30. The settlement with TJ Web Productions is the fifth after the FTC announced a crackdown on sexually explicit e−mail spam in July 2005, when the agency charged seven companies with violating a U.S. law requiring warning labels on sexually explicit e−mail. Sexually explicit e−mails sent by TJ Web affiliates have been "widely distributed" since May 2004, according to an FTC complaint.
Source: http://www.infoworld.com/article/07/01/30/HNpornspamcharges_1.html

33. *January 26, NewScientist* — **Mysterious source jams satellite communications.** Paris−based satellite company Eutelsat is investigating "unidentified interference" with its satellite broadcast services that temporarily knocked out several television and radio stations. The company

declined to say whether it thought the interference was accidental or deliberate. The problem began Tuesday afternoon, January 23, blocking several European, Middle East and northeast African radio and television stations, as well as Agence France−Presse's news service. All transferred their satellite transmissions to another frequency to resume operations. Theresa Hitchens of the Center for Defense Information think−tank in Washington, DC, says there have been cases of deliberate satellite jamming in the past, but it is hard to see what motivation there would be in this instance. "It's really puzzling to me," she said. "If it was accidental, why would they be so secretive about saying what the source was and if it's deliberate, you've got to wonder why −− it just seems to me to be an odd target..." she says.
Source: http://space.newscientist.com/article/dn11033−mysterious−source−jams−satellite−communications.html

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	The top 10 Target Ports are temporarily unavailable. We apologize for the inconvenience. Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

34. *January 31, Christian Science Monitor* — **A foiled plot in Britain may signal chilling tactic.** British security officials were claiming Wednesday, January 31, to have foiled a terrorist plot which would have imported for the first time to Britain the grisly Iraq−style tactic of kidnapping a victim, torturing and beheading him and filming the atrocity for broadcast on the Internet. In what police characterized as "the foothills of a major investigation," at least nine arrests were made at a dozen addresses in and around Birmingham, England, including homes, an Islamic bookshop, and a cybercafe. But experts said this plot's new tactic, if confirmed, would amount to a significant departure in strategy. Thus far, the public has focused its concern on the possibility of suicide bombers seeking to emulate the perpetrators of the July 7, 2005, bombings that killed 52 people. The prospect of being snatched from the street, paraded before video cameras, and decapitated was considered a horror peculiar only to countries like Iraq. "A plot to kidnap, torture, and execute an individual in the heart of England, and film the gruesome events on a videotape for posting on the Internet, represents a new chilling escalation in tactics by the global jihadi terror groups and carries grave implications for all western nations," says MJ Gohel, a terrorism expert with the London−based Asia−Pacific Foundation.

Source: http://www.csmonitor.com/2007/0201/p01s03−woeu.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer